

REMARKS

Initially, Applicants would like to thank the Examiner for withdrawing each of the previous rejections.

In the outstanding Official Action, none of the claims were rejected over prior art. However, claims 34-66 were rejected under 35 U.S.C. §112, first paragraph, as failing to comply with the written description requirement. Claims 34-66 were also rejected under 35 U.S.C. §112, second paragraph, as indefinite. Applicants traverse each of the outstanding rejections.

With respect to the rejection under 35 U.S.C. §112, first paragraph, the Official Action asserts that the original specification does not disclose storing the system security manager's certificate onto a security kernel of an operating system based upon a digital signature of the system security manager. In this regard, the Official Action acknowledges that the originally filed specification discloses generating a system security manager's certificate based upon a signature of the system security manager. Insofar as the system security manager's certificate is acknowledged to be disclosed as being generated based upon a signature of the system security manager, and insofar as the system security manager's certificate is disclosed as being stored onto a security kernel of an operating system (as explained below), there is no proper basis for the assertion that the system security manager's certificate is not disclosed as being stored onto a security kernel of an operating system based upon a digital signature of the system security manager.

As acknowledged in the Official Action, the originally filed specification discloses, at page 9, lines 25-30, generating a system security manager's certificate based upon a signature of the system security manager. Also, the originally filed specification discloses, at page 5, lines 18-

20, the security management module 214 issues a certificate based on the encryption keys and the digital signature value.

The originally filed specification further discloses, at page 5, lines 28-29, the security kernel 238 verifies the digital signature, sets and inquires the access authority of the file. Also, the originally filed specification discloses, at page 6, lines 4-11, the security kernel includes... a system security manager certificate storage 312. Finally, the originally filed specification discloses, at page 9, line 36 to page 10, line 3, the system security manager stores his/her certificate CERT\_SM onto the system security manager certificate storage 312 in the security kernel 238. Accordingly, storing the system security manager's certificate onto a security kernel of an operating system based upon a digital signature of the system security manager is disclosed in the original specification.

The Official Action further asserts that the original specification does not disclose setting an access authority of the file system for the user's digital signature keys and certificate. However, the originally filed specification discloses, with respect to Figure 9, element 918, at page 10, lines 25-29 if user's access authority ACID\_U is equal to system security manager's access authority ACID\_SM, system security manager's access authority is applied to an access authority of a user process ACID\_UP at step 910. The user process having system security manager's access authority ACID\_SM selects and executes one of a user registering/deleting process, a file system access authority setting process and a file access process at steps 914, 916, 918 and 920. Further, the originally filed specification discloses, with respect to Figure 12, elements 1204-1208, at page 13, lines 1-5, the system security manager selects users who are allowed to access the file at step 1204. The security kernel sets an access authority ACID\_F of the file selected at the step 1204 as the access authority ACID\_U of the user selected at the step

1206 at step 1208. Further, the relationship of the access authority, the public key, the secret key and the certificate for a new user is described at page 12, lines 10-22. Accordingly, setting an access authority of the file system for the user's digital signature keys and certificate is disclosed in the original specification.

With respect to the rejection under 35 U.S.C. §112, second paragraph, the Official Action asserts that the independent claims do not interrelate to those elements which are essential to the invention. However, the characterization of elements essential to the invention is entirely inappropriate and unsupported under the requirements of 35 U.S.C. §112, second paragraph. In this regard, the characterization of "the invention" appears to be an attempt to redraft the claims using exemplary features and characterizations of the disclosure which are arbitrarily deemed as "essential". Accordingly the Examiner is requested to separately identify each feature of "the invention" which is believed to be essential and not present in the pending claims, as well as a reason that such features are believed to be essential, so that Applicants are afforded a proper opportunity to either explain that such features are not essential, or to explain where in the claims such features are interrelated with other features.

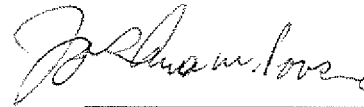
In any case, any essential elements of the present invention are properly interrelated in the claims under 35 U.S.C. §112, second paragraph. In this regard, the features of claims 34, 45 and 56 are properly interrelated, and include any features properly characterized as "essential", at least insofar as a person skilled in the art would easily acknowledge the interrelation between the claimed elements. Accordingly, reconsideration and withdrawal of the rejection under 35 U.S.C. §112, second paragraph, is respectfully requested.

SUMMARY AND CONCLUSION

Applicants have discussed the features recited in Applicants' claims and have shown that these features are entirely compliant with the requirements of 35 U.S.C. §112. Accordingly, Applicants respectfully request reconsideration and withdrawal of each of the outstanding rejections, as well as an indication of the allowability of each of the claims now pending.

Should the Examiner have any questions, please contact the undersigned at the telephone number provided below.

Respectfully submitted,  
You-Jin EUN et al.



Bruce H. Bernstein  
Reg. No. 29,027

Joshua M. Povsner  
Reg. #42,086

December 19, 2006  
GREENBLUM & BERNSTEIN, P.L.C.  
1950 Roland Clarke Place  
Reston, VA 20191  
(703) 716-1191